

CONGRUENCES BETWEEN WORD LENGTH STATISTICS FOR THE FINITARY ALTERNATING AND SYMMETRIC GROUPS

TESSA COTRON, ROBERT DICKS, AND SARAH FLEMING

ABSTRACT. In [3], Bacher and de la Harpe study conjugacy growth series of infinite permutation groups and their relationships with $p(n)$, the partition function, and $p(n)_e$, a generalized partition function. They prove identities for the conjugacy growth series of the finitary symmetric group and the finitary alternating group. The group theory in [3] also motivates an investigation into congruence relationships between the finitary symmetric group and the finitary alternating group. Using the Ramanujan congruences for the partition function $p(n)$ and Atkin's generalization to the k -colored partition function $p_k(n)$, we prove the existence of congruence relations between these two series modulo arbitrary powers of 5 and 7, which we systematically describe. Furthermore, we prove that such relationships exist modulo powers of all primes $\ell \geq 5$.

1. INTRODUCTION

In a recent paper [3], Bacher and de la Harpe study the conjugacy growth series of infinite permutation groups that are locally finite. Given $g \in G$, where G is a group generated by some set S , define the *word length* $\ell_{G,S}(g)$ as the minimal non-negative integer n where $g = s_1 s_2 \cdots s_n$ and $s_1, s_2, \dots, s_n \in S \cup S^{-1}$. They define the *conjugacy length* $\kappa_{G,S}(g)$ as the minimal integer n such that there exists an h in the conjugacy class of g for which $\ell_{G,S}(h) = n$. The number of conjugacy classes in G consisting of elements g where $\kappa_{G,S}(g) = n$ for $n \in \mathbb{N}$ is denoted $\gamma_{G,S}(n) \in \mathbb{N} \cup \{0\} \cup \{\infty\}$. If $\gamma_{G,S}(n)$ is finite for all $n \in \mathbb{N}$ for a given pair (G, S) , then the *conjugacy growth series* is defined to be

$$(1.1) \quad C_{G,S}(q) := \sum_{n=0}^{\infty} \gamma_{G,S}(n) q^n.$$

Given a permutation g of a non-empty set X , denote the *support* of g as $\text{supp}(g) := \{x \in X : g(x) \neq x\}$. The group of permutations of X with finite support is the *finitary symmetric group* $\text{Sym}(X)$. The subgroup of $\text{Sym}(X)$ with permutations of even signature is the *finitary alternating group* $\text{Alt}(X)$. Let $S \subset \text{Sym}(\mathbb{N})$ be a generating set of $\text{Sym}(\mathbb{N})$ such that $S_{\mathbb{N}}^{\text{Cox}} \subset S \subset T_{\mathbb{N}}$, where

$$(1.2) \quad S_{\mathbb{N}}^{\text{Cox}} := \{(i, i+1) : i \in \mathbb{N}\}$$

Date: July 13, 2016.

2010 Mathematics Subject Classification. 11P82, 11P83.

Key words and phrases. Partitions, finitary permutation groups, Ramanujan congruences.

is such that $(\text{Sym}(\mathbb{N}), S_{\mathbb{N}}^{\text{Cox}})$ is a Coxeter system, and

$$(1.3) \quad T_{\mathbb{N}} := \{(x, y) \in \text{Sym}(\mathbb{N}) : x, y \in \mathbb{N} \text{ are distinct}\}$$

is the conjugacy class of all transpositions in $\text{Sym}(\mathbb{N})$. Throughout this paper, we define S to be the set described above. By Proposition 1 in [3], the conjugacy growth series for the pair $(\text{Sym}(\mathbb{N}), S)$ is given by

$$(1.4) \quad C_{\text{Sym}(\mathbb{N}), S}(q) = \sum_{n=0}^{\infty} p(n)q^n = \prod_{n=1}^{\infty} \frac{1}{1-q^n},$$

where $p(n)$ denotes the usual integer partition function. Let $S' \subset \text{Alt}(\mathbb{N})$ be a generating set of $\text{Alt}(\mathbb{N})$ such that $S_{\mathbb{N}}^A \subset S' \subset T_{\mathbb{N}}^A$, where we define

$$(1.5) \quad S_{\mathbb{N}}^A := \{(i, i+1, i+2) \in \text{Alt}(\mathbb{N}) : i \in \mathbb{N}\}$$

and

$$(1.6) \quad T_{\mathbb{N}}^A := \cup_{g \in \text{Alt}(\mathbb{N})} g S_{\mathbb{N}}^A g^{-1}.$$

Throughout this paper, we define S' to be the set described above. By Proposition 11 in [3], the conjugacy growth series for the pair $(\text{Alt}(\mathbb{N}), S')$ is given by

$$(1.7) \quad \begin{aligned} C_{\text{Alt}(\mathbb{N}), S'}(q) &= \frac{1}{2} \sum_{n=0}^{\infty} p\left(\frac{n}{2}\right) q^n + \frac{1}{2} \sum_{n=0}^{\infty} p_2(n) q^n \\ &= \frac{1}{2} \prod_{n=1}^{\infty} \frac{1}{1-q^{2n}} + \frac{1}{2} \prod_{n=1}^{\infty} \frac{1}{(1-q^n)^2}, \end{aligned}$$

where $p\left(\frac{n}{2}\right) = 0$ for all odd n and $p_2(n)$ denotes the number of 2-colored partitions of n . Combining (1.4) and (1.7), we obtain

$$(1.8) \quad \begin{aligned} 2\gamma_{\text{Alt}(\mathbb{N}), S'}(2n) &= p(n) + p_2(2n) \\ &= \gamma_{\text{Sym}(\mathbb{N}), S}(n) + p_2(2n). \end{aligned}$$

The finite symmetric and alternating groups, S_n and A_n , have the property that A_n is a normal subgroup of S_n and $[S_n : A_n] = 2$, so one would naively expect a similar relationship between the finitary symmetric and alternating groups to hold. By (1.8), we see that $\gamma_{\text{Alt}(\mathbb{N}), S'}(2n)$ is one half of $\gamma_{\text{Sym}(\mathbb{N}), S}(n)$ together with a “discrepancy function,” $p_2(2n)$. In terms of size, we prove in [4] that $\gamma_{\text{Alt}(\mathbb{N}), S'}(n)$ and $\gamma_{\text{Sym}(\mathbb{N}), S}(n)$ behave differently asymptotically and do not follow the pattern of their finite counterparts. More precisely, in [4], the authors prove that as $n \rightarrow \infty$, we have that

$$(1.9) \quad \gamma_{\text{Sym}(\mathbb{N}), S}(n) \sim \frac{e^{\pi\sqrt{2n/3}}}{4n\sqrt{3}}$$

and

$$(1.10) \quad \gamma_{\text{Alt}(\mathbb{N}), S'}(n) \sim \frac{e^{2\pi\sqrt{n/3}}}{3^{\frac{3}{4}} \cdot 8n^{\frac{5}{4}}}.$$

It is natural to consider the question of congruence relations between the coefficients of the conjugacy growth series of each of these groups. By (1.8), there will exist congruences modulo powers of primes between $2\gamma_{\text{Alt}(\mathbb{N}),S'}(2n)$ and $\gamma_{\text{Sym}(\mathbb{N}),S}(n)$ whenever the “discrepancy function,” $p_2(2n)$, is equivalent to 0. In [4], we establish a method of proving congruences for generalized partition functions modulo a prime, including the following examples.

Example. For all $n \equiv 2, 3, 4 \pmod{5}$, we have that

$$2\gamma_{\text{Alt}(\mathbb{N}),S'}(2n) \equiv \gamma_{\text{Sym}(\mathbb{N}),S}(n) \pmod{5}.$$

Example. For all $n \equiv 17, 31, 38, 45 \pmod{49}$, we have that

$$2\gamma_{\text{Alt}(\mathbb{N}),S'}(2n) \equiv \gamma_{\text{Sym}(\mathbb{N}),S}(n) \pmod{7}.$$

It is natural to ask if these examples are part of a more general phenomenon and if there exists a method to determine congruences. Ramanujan stated congruences for the partition function $p(n)$ modulo powers of 5, 7, and 11, proved by Watson in [8]. In addition, Atkin proved the existence of congruences for the function $p_2(n)$ modulo powers of the primes 5, 7, and 13 in [2]. Building off of these results, we obtain congruences between the coefficients of the conjugacy growth series for these groups modulo powers of 5 and 7.

Throughout, we let $S \subset \text{Sym}(\mathbb{N})$ be a generating set of $\text{Sym}(\mathbb{N})$ such that $S_{\mathbb{N}}^{\text{Cox}} \subset S \subset T_{\mathbb{N}}$, where $S_{\mathbb{N}}^{\text{Cox}}$ and $T_{\mathbb{N}}$ are defined by (1.2) and (1.3), respectively. In addition, we let $S' \subset \text{Alt}(\mathbb{N})$ be a generating set for $\text{Alt}(\mathbb{N})$ such that $S_{\mathbb{N}}^A \subset S' \subset T_{\mathbb{N}}^A$, where $S_{\mathbb{N}}^A$ and $T_{\mathbb{N}}^A$ are defined by (1.5) and (1.6), respectively. Using this notation, we arrive at the following theorem:

Theorem 1.1. *Assume the notation above. Let $\ell = 5$ or 7 and let $j \geq 1$. Then for all $24n \equiv 1 \pmod{\ell^j}$, we have that*

$$\gamma_{\text{Alt}(\mathbb{N}),S'}(2n) \equiv \gamma_{\text{Sym}(\mathbb{N}),S}(n) \equiv 0 \pmod{\ell^{\lfloor j/2-1 \rfloor}}.$$

Example. For example, modulo 5, 25, and 125, we obtain for all $n \geq 0$ that

$$\begin{aligned} \gamma_{\text{Alt}(\mathbb{N}),S'}(2 \cdot 5^4 n + 1198) &\equiv 0 \pmod{5} \\ \gamma_{\text{Alt}(\mathbb{N}),S'}(2 \cdot 5^6 n + 29948) &\equiv 0 \pmod{25} \\ \gamma_{\text{Alt}(\mathbb{N}),S'}(2 \cdot 5^8 n + 748698) &\equiv 0 \pmod{125}. \end{aligned}$$

Likewise, modulo 7, 49, and 343, we obtain for all $n \geq 0$ that

$$\begin{aligned} \gamma_{\text{Alt}(\mathbb{N}),S'}(2 \cdot 7^4 n + 4602) &\equiv 0 \pmod{7} \\ \gamma_{\text{Alt}(\mathbb{N}),S'}(2 \cdot 7^6 n + 225494) &\equiv 0 \pmod{49} \\ \gamma_{\text{Alt}(\mathbb{N}),S'}(2 \cdot 7^8 n + 11049202) &\equiv 0 \pmod{343}. \end{aligned}$$

It is a natural question to ask what holds for general primes $\ell \notin \{5, 7\}$. Following the work of Treneer [7], we prove the existence of congruences between the coefficients of the conjugacy growth series for $(\text{Alt}(\mathbb{N}), S')$ and $(\text{Sym}(\mathbb{N}), S)$ modulo

arbitrary powers of primes $\ell \geq 5$. Treneer's work gives general congruences for coefficients of various types of modular forms. Here, we follow her method and make it explicit.

Let $\ell \geq 5$ be prime. We then define

$$(1.11) \quad m_\ell := \begin{cases} 2 & 5 \leq \ell \leq 23 \\ 1 & \ell \geq 29, \end{cases}$$

$$(1.12) \quad \delta_\ell := \frac{Q^{\ell^{m_\ell}} \beta_\ell + 1}{24},$$

and

$$(1.13) \quad \beta_\ell := \frac{23}{Q^{\ell^{m_\ell}}} \pmod{24}.$$

Using this notation, we arrive at the following theorem:

Theorem 1.2. *Assume the above notation. Let $\ell \geq 5$ be prime and let $j \geq 1$. Then for a positive proportion of primes $Q \equiv -1 \pmod{144\ell^j}$, we have that*

$$2\gamma_{\text{Alt}(\mathbb{N}), S'}(2Q\ell^{m_\ell}n + 2\delta_\ell) \equiv \gamma_{\text{Sym}(\mathbb{N}), S}(Q\ell^{m_\ell}n + \delta_\ell) \pmod{\ell^j}$$

for all $24n + \beta_\ell$ coprime to $Q\ell$.

In this paper, we make effective the effort of [7] by focusing on the specific case of the function $p_2(n)$, which arises from the conjugacy growth series for $(\text{Alt}(\mathbb{N}), S')$. We use properties of modular forms to prove the existence of congruences between the coefficients of these two series.

Section 2.1 covers the basics of modular forms and cusps, and Section 2.2 focuses on congruences for the partition function $p(n)$ and the k -colored partition function $p_k(n)$ modulo prime powers. In Section 2.3 we state a theorem of Serre. Section 3 provides a proof of Theorem 1.1 using the Ramanujan and Atkin congruences. In Section 4, we focus on and make effective a special case of Theorem 1.2 in [7], which we require in order to prove the existence of congruences between $2\gamma_{\text{Alt}(\mathbb{N}), S'}(2n)$ and $\gamma_{\text{Sym}(\mathbb{N}), S}(n)$. In Section 5, we use this result to prove Theorem 1.2.

ACKNOWLEDGMENTS

The authors would like to thank Ken Ono and Olivia Beckwith for advising this project and for their many helpful conversations and suggestions. In addition, the authors would like to thank Emory University and the NSF for their support via grant DMS-1250467.

2. PRELIMINARIES

Here we state standard properties of modular forms that can be found in many texts such as [1] and [6].

2.1. Modularity, Cusps, and Operators. The proof of Theorem 1.2 uses properties of modular forms, which requires the understanding of cusps. A *cusp* of $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ is an equivalence class in $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$ under the action of Γ [6, p. 2]. We use the following definition of modular forms from [1, p. 114]:

Definition 2.1. A function f is said to be an *entire modular form of weight k* on a subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ if it satisfies the following conditions:

- (i) f is analytic in the upper-half \mathbb{H} of the complex plane,
- (ii) f satisfies the equation

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$$

whenever $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ and $z \in \mathbb{H}$, and

- (iii) the Fourier expansion of f has the form

$$f(z) = \sum_{n=0}^{\infty} c(n) e^{2\pi i n z}$$

at the cusp $i\infty$, and f has analogous Fourier expansions at all other cusps.

In particular, we study *Dedekind's eta-function*, a weight $1/2$ modular form defined as the infinite product

$$\eta(z) := q^{1/24} \prod_{n=1}^{\infty} (1 - q^n),$$

where $q := e^{2\pi i z}$ and $z \in \mathbb{H}$. An *eta-quotient* is a function $f(z)$ of the form

$$f(z) := \prod_{\delta|N} \eta(\delta z)^{r_\delta},$$

where $N \geq 1$ and each r_δ is an integer. If each $r_\delta \geq 0$, then $f(z)$ is known as an *eta-product*.

If N is a positive integer, then we define $\Gamma_0(N)$ as the congruence subgroup

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \pmod{N} \right\}.$$

We recall Theorem 1.64 from [6, p. 18] regarding the modularity of eta-quotients:

Proposition 2.2. *If $f(z) = \prod_{\delta|N} \eta(\delta z)^{r_\delta}$ has integer weight $k = \frac{1}{2} \sum_{\delta|N} r_\delta$, with the additional properties that*

$$\sum_{\delta|N} \delta r_\delta \equiv 0 \pmod{24}$$

and

$$\sum_{\delta|N} \frac{N}{\delta} r_\delta \equiv 0 \pmod{24},$$

then $f(z)$ satisfies

$$(2.1) \quad f\left(\frac{az+b}{cz+d}\right) = \chi(d)(cz+d)^k f(z)$$

for every $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ where the character χ is defined by $\chi(d) := \left(\frac{(-1)^k s}{d}\right)$, where $s := \prod_{\delta|N} \delta^{r_\delta}$.

Any modular form that is holomorphic (resp. vanishes) at all cusps of $\Gamma_0(N)$ and satisfies (2.1) is said to have Nebentypus character χ , and the space of such forms is denoted $M_k(\Gamma_0(N), \chi)$ (resp. $S_k(\Gamma_0(N), \chi)$). In particular, if k is a positive integer and $f(z)$ satisfies the conditions of Proposition 2.2 and is holomorphic (resp. vanishes) at all of the cusps of $\Gamma_0(N)$, then $f(z) \in M_k(\Gamma_0(N), \chi)$ (resp. $S_k(\Gamma_0(N), \chi)$). If $f(z)$ satisfies the conditions of Proposition 2.2 but has poles at the cusps of $\Gamma_0(N)$, then we say $f(z)$ is a *weakly holomorphic modular form*, and the space of such forms is denoted $M_k^!(\Gamma_0(N), \chi)$.

If $f(z)$ is a modular form, then we can act on it with various types of operators. If $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, then the action of the *slash operator* $|_k$ on $f(z)$ is defined by

$$(f|_k \gamma)(z) := (cz+d)^{-k} f(\gamma z),$$

where

$$\gamma z := \frac{az+b}{cz+d}.$$

Next, we define

$$(2.2) \quad \sigma_{v,t} := \begin{pmatrix} 1 & v \\ 0 & t \end{pmatrix}.$$

If $f(z) = \sum_{n=n_0}^{\infty} a(n)q^n$ is a weight k modular form, then the action of the *U-operator* $U(d)$ on $f(z)$ is defined by

$$f(z)|U(d) := t^{\frac{k}{2}-1} \sum_{v=0}^{t-1} f(z)|_k \sigma_{v,t} = \sum_{n=n_0}^{\infty} a(dn)q^n.$$

Likewise, the action of the *V-operator* $V(d)$ is defined by

$$f(z)|V(d) := t^{-\frac{k}{2}} f(z)|_k \begin{pmatrix} t & 0 \\ 0 & 1 \end{pmatrix} = \sum_{n=n_0}^{\infty} a(n)q^{dn}.$$

Now, if $f(z) = \sum_{n=0}^{\infty} a(n)q^n \in M_k(\Gamma_0(N), \chi)$, then the action of the *Hecke operator* $T_{p,k,\chi}$ on $f(z)$ is defined by

$$f(z)|T_{p,k,\chi} := \sum_{n=0}^{\infty} (a(pn) + \chi(p)p^{k-1}a(n/p))q^n,$$

where $a(n/p) = 0$ if $p \nmid n$. We recall the following result from [6, p. 21,28]:

Proposition 2.3. *Suppose that $f(z) \in M_k(\Gamma_0(N), \chi)$.*

(1) If $d \mid N$, then

$$f(z) \mid U(d) \in M_k(\Gamma_0(N), \chi).$$

(2) If d is a positive integer, then

$$f(z) \mid V(d) \in M_k(\Gamma_0(Nd), \chi).$$

(3) If $p \geq 2$, then

$$f(z) \mid T_{p,k,\chi} \in M_k(\Gamma_0(N), \chi).$$

2.2. Ramanujan's Congruences and Atkin's Generalizations. Ramanujan conjectured the following congruences for the partition function modulo powers of the primes 5 and 7, which Watson proved in [8].

Theorem 2.4 (Ramanujan). *Let $\ell = 5, 7$, or 11 and let $j \geq 1$. Then if $24n \equiv 1 \pmod{\ell^j}$, we have that*

$$\begin{cases} p(n) \equiv 0 \pmod{\ell^j} & \ell = 5, 11 \\ p(n) \equiv 0 \pmod{\ell^{\lfloor j/2 \rfloor + 1}} & \ell = 7. \end{cases}$$

In [2], Atkin generalized the Ramanujan congruences modulo powers of 5, 7, and 11 to the function $p_k(n)$, which counts the number of k -colored partitions of n .

Theorem 2.5 (Atkin). *Let $k > 0$, $\ell = 2, 3, 5, 7$ or 13, and $j \geq 1$. Then if $24n \equiv k \pmod{\ell^j}$, we have that*

$$p_k(n) \equiv 0 \pmod{\ell^{\lfloor \alpha j/2 + \epsilon \rfloor}},$$

where $\epsilon := \epsilon(k) = O(\log k)$ and $\alpha = \alpha(k, \ell)$ depending on ℓ and the residue of k modulo 24.

Atkin computes the value of $\alpha(k, \ell)$ in a table in [2]. We note the following values of α :

$$(2.3) \quad \alpha(2, 5) = \alpha(2, 7) = 1.$$

In addition, following Atkin's method to calculate ϵ exactly, we observe

$$(2.4) \quad \epsilon = \begin{cases} 1 - \lfloor \log(48)/\log(\ell) \rfloor = -1 & \ell = 5 \\ -\lfloor \log(48)/\log(\ell) \rfloor = -1 & \ell = 7. \end{cases}$$

Therefore, for the case where $k = 2$ and $\ell = 5$ or 7, we have that for all $24n \equiv k \pmod{\ell^j}$,

$$(2.5) \quad p_2(n) \equiv 0 \pmod{\ell^{\lfloor j/2 - 1 \rfloor}}.$$

2.3. Serre's Theorem. We make use of the following theorem of Serre's regarding congruences for certain types of modular forms, stated in [7]:

Theorem 2.6 (Serre). *Suppose that $f(z) = \sum_{n=1}^{\infty} a(n)q^n \in S_k(\Gamma_0(N), \chi)$ has coefficients in the ring of integers \mathcal{O}_K of a number field K and M is a positive integer. Furthermore, suppose that $k \geq 1$. Then a positive proportion of the primes $p \equiv -1 \pmod{MN}$ have the property that*

$$f(z) \mid T_{p,k,\chi} \equiv 0 \pmod{M}.$$

Serre's theorem guarantees the existence of congruences for cusp forms with coefficients in the ring of integers of a number field, which we will use to prove properties of the coefficients of the conjugacy growth series for $(\text{Alt}(\mathbb{N}), S')$ and $(\text{Sym}(\mathbb{N}), S)$.

3. PROOF OF THEOREM 1.1

We first prove congruences for arbitrary powers of $\ell = 5$ or 7 . Let $j \geq 1$ and suppose that $24n \equiv 1 \pmod{\ell^j}$. Then by Theorem 2.4, we have that

$$(3.1) \quad \gamma_{\text{Sym}(\mathbb{N}), S}(n) = p(n) \equiv 0 \pmod{\ell^{\lfloor j/2 \rfloor + 1}}.$$

Additionally, we have that $24(2n) \equiv 2 \pmod{\ell^j}$. Using the case of Theorem 2.5 where $k = 2$ and $\ell = 5$ or 7 , as in (2.5), we have that

$$(3.2) \quad p_2(2n) \equiv 0 \pmod{\ell^{\lfloor j/2 - 1 \rfloor}}.$$

Therefore, for all $24n \equiv 1 \pmod{\ell^j}$, we obtain from (1.8), (3.1), and (3.2) that

$$(3.3) \quad \gamma_{\text{Alt}(\mathbb{N}), S'}(2n) \equiv \gamma_{\text{Sym}(\mathbb{N}), S}(n) \equiv 0 \pmod{\ell^{\lfloor j/2 - 1 \rfloor}},$$

as desired. \square

4. CONGRUENCES FOR $p_2(n)$

Because of the relationship between the conjugacy growth series for $(\text{Alt}(\mathbb{N}), S')$ and the function $p_2(n)$, here, we focus on congruences for $p_2(n)$. By the definition of the 2-colored partition function $p_2(n)$, we have that

$$(4.1) \quad \sum_{n=0}^{\infty} p_2(n) q^n = \prod_{n=1}^{\infty} \frac{1}{(1 - q^n)^2} = \frac{q^{\frac{1}{12}}}{\eta^2(z)}.$$

Throughout, we let

$$(4.2) \quad f(z) := \frac{1}{\eta(12z)^2} = \sum_{n=-1}^{\infty} a(n) q^n.$$

Then we have that $p_2\left(\frac{n+1}{12}\right) = a(n)$. In order to prove congruences between the coefficients of the conjugacy growth series for $(\text{Alt}(\mathbb{N}), S')$ and $(\text{Sym}(\mathbb{N}), S)$, we first prove a theorem concerning the coefficients of $f(z)$. This makes effective the following result of Treneer [7] by determining the exact value of m that is sufficiently large.

Proposition 4.1 (Treneer). *Suppose that ℓ is an odd prime and that k and m are integers. Let N be a positive integer with $(N, p) = 1$, and let χ be a Dirichlet character modulo N . Let K be an algebraic number field with ring of integers \mathcal{O}_K , and suppose $f(z) = a(n)q^n \in M_k^1(\Gamma_0(N), \chi) \cap \mathcal{O}_K((q))$. If m is sufficiently large, then for each positive integer j , a positive proportion of the primes $Q \equiv -1 \pmod{N\ell^j}$ have the property that*

$$a(Q\ell^m n) \equiv 0 \pmod{\ell^j}$$

for all n coprime to $Q\ell$.

This section closely follows Section 3 in [7]. Throughout this section, let $f(z)$ be defined by (4.2).

Theorem 4.2. *Let $\ell \geq 5$ be prime and $j \in \mathbb{N}$. Then for a positive proportion of primes $Q \equiv -1 \pmod{144\ell^j}$, we have that*

$$a(Q\ell^{m_\ell}n) \equiv 0 \pmod{\ell^j}$$

for all n coprime to $Q\ell$.

The proof of Theorem 4.2 requires the construction of a cusp form that preserves congruence properties of the function $f(z)$.

Proposition 4.3. *For every positive integer j , there exists an integer $\beta \geq j-1$ and a cusp form*

$$g_{\ell,j}(z) \in S_\kappa(\Gamma_0(144\ell^2), \chi) \cap \mathbb{Z}((q)),$$

where $\kappa := -1 + \frac{\ell^\beta(\ell^2-1)}{2}$, with the property that

$$g_{\ell,j}(z) \equiv \sum_{n=1}^{\infty} a(\ell^{m_\ell}n)q^n \pmod{\ell^j}.$$

We first require the following proposition concerning the Fourier expansion of $f(z)$ at a given cusp after being acted on by the $U(\ell^m)$ operator for $m \geq 1$.

Proposition 4.4. *Let $\gamma := \begin{pmatrix} a & b \\ c\ell^2 & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ where $c \in \mathbb{Z}$ and $ac > 0$. Then there exists an integer $n_0 \geq -24$ and a sequence $\{a_0(n)\}_{n \geq n_0}$ such that for each $m \geq 1$, we have that*

$$(f(z) | U_{\ell^m}) |_{-1} \gamma = \sum_{\substack{n=n_0 \\ n \equiv 0 \pmod{\ell^m}}}^{\infty} a_0(n) q_{24\ell^m}^n,$$

where $q_{24\ell^m} := e^{\frac{2\pi iz}{24\ell^m}}$.

The proof of this proposition makes use of the following lemma, which relies on the proof of Theorem 1 in [5].

Lemma 4.5. *Given any matrix $A \in \mathrm{SL}_2(\mathbb{Z})$, we have that*

$$f(z) |_{-1} A = \sum_{n=n_0}^{\infty} a_0(n) q_{24}^n$$

where $a_0(n) \in \mathbb{Z}$ and $n_0 \geq -24$.

Proof. Let $A := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. Then, as in the proof of Theorem 1 in [5], we can write

$$(4.3) \quad \begin{pmatrix} 12 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix}$$

where $\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, $\alpha, \beta, \delta \in \mathbb{Z}$, and $\alpha, \delta > 0$. Then we have that $12a = a'\alpha$ and $c = c'\alpha$, so $\alpha = (a'\alpha, c'\alpha) = (12a, c) = (12, c) \leq 12$. Again, by Theorem 1 in [5], we obtain

$$(4.4) \quad f(z) \mid_{-1} A = \sum_{n=n_0}^{\infty} a_0(n) q_{24}^n$$

where $n_0 := \frac{-2\alpha}{\delta} > -2\alpha \geq -24$. \square

Proof of Proposition 4.4. As in [7], for each $0 \leq v \leq \ell^m - 1$, choose an integer s_v such that

$$(4.5) \quad s_v N \equiv (a + vc\ell^2)^{-1}(b + vd) \pmod{\ell^m}$$

and define $w_v := s_v N$. We let

$$(4.6) \quad \alpha_0 := \begin{pmatrix} a & 0 \\ c\ell^{m+2} & d - w_0 c\ell^2 \end{pmatrix}.$$

By (2.1), we have that

$$(4.7) \quad (f(z) \mid U_{\ell^m}) \mid_{-1} \gamma = (\ell^m)^{-\frac{3}{2}} \sum_{v=0}^{\ell^m-1} f(z) \mid_{-1} \sigma_{v, \ell^m} \gamma.$$

We observe that $\sigma_{v, \ell^m} \gamma = \alpha_0 \sigma_{w_v, \ell^m}$, so we have that

$$(4.8) \quad (f(z) \mid U_{\ell^m}) \mid_{-1} \gamma = (\ell^m)^{-\frac{3}{2}} \sum_{v=0}^{\ell^m-1} f(z) \mid_{-1} \alpha_0 \sigma_{w_v, \ell^m}.$$

By Lemma 4.5, we have that

$$f(z) \mid_{-1} \alpha_0 = \sum_{n=n_0}^{\infty} a_0(n) q_{24}^n,$$

so we obtain

$$(4.9) \quad \begin{aligned} \sum_{v=0}^{\ell^m-1} f(z) \mid_{-1} \alpha_0 \sigma_{w_v, \ell^m} &= \sum_{v=0}^{\ell^m-1} \ell^{\frac{m}{2}} \sum_{n=n_0}^{\infty} a_0(n) e^{\frac{2\pi i n(z+w_v)}{24\ell^m}} \\ &= \ell^{\frac{m}{2}} \sum_{n=n_0}^{\infty} a_0(n) q_{24\ell^m}^n \sum_{v=0}^{\ell^m-1} e^{\frac{2\pi i n w_v}{24\ell^m}}. \end{aligned}$$

By Lemma 3.3 in [7], the numbers $\frac{w_v}{24}$ run through the residue classes modulo ℓ^m as v does. Therefore, we have that

$$(4.10) \quad \sum_{v=0}^{\ell^m-1} e^{\frac{2\pi i n w_v}{24\ell^m}} = \sum_{v=0}^{\ell^m-1} e^{\frac{2\pi i n v}{\ell^m}} = \begin{cases} \ell^m & n \equiv 0 \pmod{\ell^m} \\ 0 & \text{else.} \end{cases}$$

Combining (4.9) and (4.10), we have that

$$(4.11) \quad \sum_{v=0}^{\ell^m-1} f(z) \big|_{-1} \alpha_0 \sigma_{w_v, \ell^m} = \ell^{\frac{3}{2}} \sum_{\substack{n=n_0 \\ n \equiv 0 \pmod{\ell^m}}}^{\infty} a_0(n) q_{24\ell^m}^n.$$

Using (4.7) and (4.11), we obtain

$$(4.12) \quad (f(z) \big| U_{\ell^m}) \big|_{-1} \gamma = \sum_{\substack{n=n_0 \\ n \equiv 0 \pmod{\ell^m}}}^{\infty} a_0(n) q_{24\ell^m}^n,$$

the Fourier expansion of $f(z) \big| U_{\ell^m}$ at the cusp $\frac{a}{c\ell^2}$. \square

We now construct a weakly holomorphic modular form which vanishes at certain cusps of $\Gamma_0(144\ell^2)$.

Proposition 4.6. *For each nonnegative integer m , define*

$$f_m(z) := f(z) \big| U_{\ell^m} - f(z) \big| U_{\ell^{m+1}} \big| V_{\ell} \in M_{-1}^!(\Gamma_0(144\ell^2), \chi).$$

Then $f_{m_{\ell}}$ vanishes at each cusp $\frac{a}{c\ell^2}$ of $\Gamma_0(144\ell^2)$ with $ac > 0$.

Proof. By Proposition 4.4, we have that

$$(4.13) \quad (f(z) \big| U_{\ell^{m_{\ell}}}) \big| \gamma = \sum_{\substack{n=n_0 \\ n \equiv 0 \pmod{\ell^{m_{\ell}}}}}^{\infty} a_0(n) q_{24\ell^{m_{\ell}}}^n$$

where $n_0 \geq -24$. We now consider two cases. If $5 \leq \ell \leq 23$, we have that

$$-\ell^{m_{\ell}} \leq -25 < -24 \leq n_0,$$

and if $\ell \geq 29$, we have that

$$-\ell^{m_{\ell}} \leq -29 < -24 \leq n_0.$$

Suppose $a_0(n) \neq 0$. Then $n \geq n_0 > -\ell^{m_{\ell}}$, but $n \equiv 0 \pmod{\ell^{m_{\ell}}}$, so $n \geq 0$. Therefore, we obtain

$$(4.14) \quad (f(z) \big| U_{\ell^{m_{\ell}}}) \big| \gamma = \sum_{\substack{n=0 \\ n \equiv 0 \pmod{\ell^{m_{\ell}}}}}^{\infty} a_0(n) q_{24\ell^{m_{\ell}}}^n$$

so $f(z) \big| U_{\ell^{m_{\ell}}}$ is holomorphic at the cusp $\frac{a}{c\ell^2}$.

Now, by Proposition 3.5 in [7], we have that

$$(4.15) \quad f_m(z) \big|_{-1} \gamma = \sum_{\substack{n=0 \\ n \equiv 0 \pmod{\ell^m}}}^{\infty} a_0(n) q_{24\ell^m}^n - \sum_{\substack{n=0 \\ n \equiv 0 \pmod{\ell^{m+1}}}}^{\infty} a_0(n) q_{24\ell^m}^n,$$

so the constant term in each expansion is $a_0(0)$, and they cancel. Therefore, $f_{m_{\ell}}$ vanishes at the cusp $\frac{a}{c\ell^2}$. \square

We are now ready to prove Proposition 4.3.

Proof of Proposition 4.3. As in [7], we define the eta-quotient

$$(4.16) \quad F_\ell(z) := \frac{\eta^{\ell^2}(z)}{\eta(\ell^2 z)} \in M_{\frac{\ell^2-1}{2}}(\Gamma_0(\ell^2)).$$

By Theorem 1.65 in [6], we see that F_ℓ vanishes at every cusp $\frac{a}{c}$ of $\Gamma_0(144\ell^2)$ with $\ell^2 \nmid c$. We also have that $F_\ell(z)^{\ell^{s-1}} \equiv 1 \pmod{\ell^s}$ for any integer $s \geq 1$.

Now, define

$$(4.17) \quad g_{\ell,j}(z) := f_{m_\ell}(z) \cdot F_\ell(z)^{\ell^\beta}$$

where $\beta \geq j-1$ is sufficiently large such that $g_{\ell,j}(z)$ vanishes at all cusps $\frac{a}{c}$ of $\Gamma_0(144\ell^2)$ where $\ell^2 \nmid c$. By Theorem 1.65 in [6], it is possible to choose such a β such that the order of vanishing of $g_{\ell,j}(z)$ is at least one at all such cusps. Then $g_{\ell,j} \in \mathbb{Z}((q))$ and

$$(4.18) \quad g_{\ell,j}(z) \equiv f_{m_\ell}(z) \pmod{\ell^j}.$$

By our choice of β , $g_{\ell,j}(z)$ vanishes at all cusps $\frac{a}{c}$ of $\Gamma_0(144\ell^2)$ where $\ell^2 \nmid c$. Furthermore, by Proposition 4.6, $g_{\ell,j}(z)$ vanishes at all cusps $\frac{a}{c}$ where $\ell^2 \mid c$. Define $\kappa := -1 + \frac{\ell^\beta(\ell^2-1)}{2}$. Then we have that

$$(4.19) \quad g_{\ell,j}(z) \in S_\kappa(\Gamma_0(144\ell^2), \chi).$$

By definition of f_{m_ℓ} , we obtain

$$(4.20) \quad g_{\ell,j}(z) \equiv \sum_{n=1}^{\infty} a(\ell^{m_\ell} n) q^n - \sum_{n=1}^{\infty} a(\ell^{m_\ell+1} n) q^n \equiv \sum_{\substack{n=1 \\ \ell \nmid n}}^{\infty} a(\ell^{m_\ell} n) q^n \pmod{\ell^j}.$$

Thus $g_{\ell,j}$ satisfies the conditions of Proposition 4.3. \square

Now that we have constructed the necessary cusp form, we arrive at the proof of Theorem 4.2.

Proof of Theorem 4.2. By Proposition 4.3, we can construct a cusp form $g_{\ell,j} \in S_\kappa(\Gamma_0(144\ell^2), \chi) \in \mathbb{Z}((q))$ such that

$$(4.21) \quad g_{\ell,j}(z) \equiv \sum_{\substack{n=1 \\ \ell \nmid n}}^{\infty} a(\ell^{m_\ell} n) q^n \pmod{\ell^j}.$$

By Theorem 2.6, for a positive proportion of the primes $Q \equiv -1 \pmod{144\ell^{j+2}}$, we have that

$$(4.22) \quad g_{\ell,j}(z) \mid T_{Q,\kappa,\chi}(Q) \equiv 0 \pmod{\ell^j}.$$

We can then write $g_{\ell,j}(z) = \sum_{n=1}^{\infty} b(n) q^n$ to obtain

$$(4.23) \quad g_{\ell,j}(z) \mid T_{Q,\kappa,\chi} = \sum_{n=1}^{\infty} (b(Qn) + \chi(Q) Q^{\kappa-1} b(n/Q)) q^n \equiv 0 \pmod{\ell^j}.$$

If $(Q, n) = 1$, then the coefficient of q^n in (4.23) is $b(Qn)$, so

$$(4.24) \quad a(Q\ell^{m_\ell}n) \equiv b(Qn) \equiv 0 \pmod{\ell^j}$$

for all n coprime to $Q\ell$. □

5. PROOF OF THEOREM 1.2

We now make use of Theorem 4.2 to prove congruences between the coefficients of the conjugacy growth series for $(\text{Alt}(\mathbb{N}), S')$ and $(\text{Sym}(\mathbb{N}), S)$.

Proof of Theorem 1.2. By (1.8), it is enough to show that $p_2(2Q\ell^{m_\ell}n + 2\delta_\ell) \equiv 0 \pmod{\ell^j}$. By (4.1) and (4.2), we observe $p_2\left(\frac{n+1}{12}\right) = a(n)$, so it suffices to prove the existence of congruences for $a(n)$.

By Theorem 4.2, for a positive proportion of primes $Q \equiv -1 \pmod{144\ell^j}$, we have that

$$(5.1) \quad p_2\left(\frac{Q\ell^{m_\ell}n + 1}{12}\right) = a(Q\ell^{m_\ell}n) \equiv 0 \pmod{\ell^j}$$

for all n coprime to $Q\ell$. Defining δ_ℓ and β_ℓ by (1.12) and 1.13), respectively, we can rewrite the left-hand side of equation (5.1) as

$$(5.2) \quad p_2(2Q\ell^{m_\ell}n + 2\delta_\ell)$$

for all $24n + \beta_\ell$ coprime to $Q\ell$. Therefore, for a positive proportion of primes $Q \equiv -1 \pmod{144\ell^j}$, we have that

$$(5.3) \quad p_2(2Q\ell^{m_\ell}n + 2\delta_\ell) \equiv 0 \pmod{\ell^j},$$

so we obtain

$$2\gamma_{\text{Alt}(\mathbb{N}), S'}(2Q\ell^{m_\ell}n + 2\delta_\ell) \equiv \gamma_{\text{Sym}(\mathbb{N}), S}(Q\ell^{m_\ell}n + \delta_\ell) \pmod{\ell^j},$$

as desired. □

REFERENCES

- [1] T. Apostol, *Modular functions and Dirichlet series in number theory*, Springer-Verlag, New York (1990).
- [2] A.O.L. Atkin, *Ramanujan congruences for $p_{-k}(n)$* , *Canad. J. Math* **21** (1968), no. 256, 67–78.
- [3] R. Bacher and P. de la Harpe, *Conjugacy growth series of some infinitely generated groups*, arxiv:1603.07943 [math.GR] (2016).
- [4] T. Cotroneo, R. Dicks, and S. Fleming, *Asymptotics and congruences for partition functions which arise from finitary permutation groups*, arXiv:1606.09074 [math.NT] (2016).
- [5] T. Honda and I. Miyawaki, *Zeta-functions of elliptic curves of 2-power conductor*, *Journal of the Mathematical Society of Japan* **26** (1974), no. 2, 362–373.
- [6] K. Ono, *The web of modularity: Arithmetic of the coefficients of modular forms and q -series*, AMS and CBMS, Providence, RI **102** (2004).
- [7] S. Treneer, *Congruences for the coefficients of weakly holomorphic modular forms*, *Proc. London Math. Soc.* **93** (2006), no. 2, 304–324.
- [8] G.N. Watson, *Ramanujan's Vermutung über Zerfallungszahlen*, *J. Reine Angew. Math.* **179** (1938), 97–128.

605 ASBURY CIRCLE, BOX 122042, ATLANTA, GA 30322

E-mail address: `tessa.cotron@emory.edu`

605 ASBURY CIRCLE, ATLANTA, GA 30322

E-mail address: `rdicks@emory.edu`

1192 PARESKY CENTER, WILLIAMS COLLEGE, WILLIAMSTOWN, MA 01267

E-mail address: `smf1@williams.edu`